AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

United States of America
v.
Gary Anthony Medeiros

Case No.

Defendant(s)

CRIMINAL COMPLAINT
BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of March 2022 - January 2023 in the county of Washington in the _____ District of Oregon, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2)	Receipt of Child Pornography

This criminal complaint is based on these facts:

See attached affidavit by HSI Special Agent Clinton Lindsly.

☒ Continued on the attached sheet.

/s/ Clinton Lindsly by Telephone
Complainant's signature

Clinton Lindsly, Special Agent, HSI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at 4:20 pm a.m./p.m.

Date: October 25, 2023

Youlee Yim You
Judge's signature

City and state: Portland, Oregon

Hon. Youlee Yim You, U.S. Magistrate Judge
Printed name and title

DISTRICT OF OREGON, ss: AFFIDAVIT OF CLINTON LINDSLY

Affidavit in Support of a Criminal Complaint and Arrest Warrant

I, Clinton Lindsly, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I have been employed as a Special Agent (SA) by the U.S. Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI) since August 2010. I am currently assigned to the child exploitation unit in the HSI office in Portland, Oregon. Previously, I was assigned to the HSI office in Los Angeles, California, where I worked for over six years in a money laundering and narcotics group that specialized in undercover operations. In 2018, I transferred to HSI Portland and continued to specialize in money laundering and narcotics investigations until January 2020. My formal law enforcement training includes successfully completing the 23-week HSI basic training course at the Federal Law Enforcement Training Center in Glynco, Georgia. During that training, I learned how to conduct child exploitation investigations. Since then, I have been involved in many child exploitation investigations and have assisted federal and state partners during their investigations. As such, I have become familiar with ways that child pornography is shared, distributed, and/or produced, including the use of various social media websites (Facebook, Twitter, Kik, Snapchat, Discord, Skype, etc.), "cloud" based storage, and "peer-to-peer" (P2P) networks. Often, individuals involved in child exploitation will collect or store images and/or videos on various media devices they keep at their residences, or in offsite locations such as "cloud" based storage. I have also become familiar with jargon or slang terms that people involved in child exploitation will use to discuss their activities. Additionally, I have become

familiar with how child pornography is sold, traded, and distributed on the "dark net," often being purchased with digital currency such as Bitcoin, Ripple, and others.

2. I have worked with agents involved in numerous investigations involving the sexual exploitation of children or the distribution, receipt, and possession of child pornography. I have participated in searches of premises and assisted in gathering evidence pursuant to search warrants in multiple child pornography investigations. I have participated in interviews of persons who possess, distribute, and produce child pornography.

3. I have participated in online undercover communications using messaging platforms with hundreds of people interested in the production, distribution, and receipt of child pornography. In my undercover role, I have assisted in the administration of private chat groups dedicated to the production, distribution, and receipt of child pornography. As such, I have become familiar with platforms used to facilitate the production, distribution, and receipt of child pornography and their purposes.

4. I submit this affidavit in support of a criminal complaint and arrest warrant for **Gary Anthony MEDEIROS**, for violations of 18 U.S.C. § 2252A(a)(2) – *Receipt of Child Pornography*, hereinafter the "**Target Offense**." As set forth below, there is probable cause to believe, and I do believe, that **MEDEIROS** committed the **Target Offense** between at least March 2022 and February 2023.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested criminal complaint and arrest warrant and does not set forth all my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation,

including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

6. *Title 18, United States Code, Section 2252A(a)(2)* makes it a crime to knowingly receive or distribute any child pornography using any means or facility of interstate or foreign commerce, or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.

7. The term "child pornography" is defined in 18 U.S.C. § 2256(8). "Child pornography," as defined in 18 U.S.C. § 2256(8), includes any visual depiction of a child under the age of 18 years engaging in sexually explicit conduct. "Sexually explicit conduct" is defined in 18 U.S.C. § 2256(2) and includes sexual intercourse, whether genital-genital, oral-genital, anal-genital, or oral-anal, whether between members of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; and the lascivious exhibition of the genitals, anus, or pubic area of any person.

Information Regarding Instagram

8. Instagram operates a free-access social-networking website of the same name that can be accessed at http://www.instagram.com. Instagram is now owned and operated by Facebook. Instagram allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and other information. Users can access Instagram through the Instagram website or by using a special electronic application created by the company that allows users to access the service through a mobile device. When a user utilizes

the Instagram app, geolocation and/or real-time GPS location data from the user's phone is often shared with Instagram.

9. Instagram permits users to post photos to their profiles and share photos with others on Instagram, as well as certain other social-media services, including Flickr, Facebook, and Twitter. When posting or sharing a photo on Instagram, a user can add 1) a caption to the photo; 2) various "tags" to the photo that can be used to search for the photo (e.g., a user may add the tag #vw to a photo so that people interested in Volkswagen vehicles can search for and find the photo); 3) location information to the photo, and; 4) other information to the photo. An Instagram user can also apply a variety of "filters" or other visual effects that can be used to modify the look of the posted photos. In addition, Instagram allows users to make comments on posted photos, including photos that the user posts or photos posted by other users of Instagram. Users can also "like" photos.

10. Upon creating an Instagram account, an Instagram user must create a unique Instagram username and an account password. Instagram asks users to provide basic identity and contact information upon registration and allows users to provide additional identity information for their user profile. This information may include the user's full name, email address(es), and phone number(s), as well as other personal information provided directly by the user to Instagram. This personal information is self-reported and is not "verified" by Instagram. Once an account is created, users may also adjust various privacy and account settings for their Instagram account.

11. Instagram allows users to have "Close Friends," which are other individuals with whom the user can share information without making the information public. Close Friends on

Instagram may come from contact lists maintained by the user, other third-party social media websites, and/or information or searches conducted by the user on Instagram profiles.

12. Instagram also allows users to "follow" another user, which means that they receive updates about posts made by the other user. Users may also "unfollow" other users, that is, stop following the other user. Users may also block other users, which prevents the other users from following them.

13. Instagram allow users to post and share various types of user content, including photos, comments, and other materials. Additionally, Instagram users can directly communicate via private message with other Instagram users. Users on Instagram may also search Instagram for other users or specific types of photos or other content.

Background on Mega

14. Mega or Mega NZ is an encrypted cloud-based storage and file hosting service offered by Mega Limited, a company based in Auckland, New Zealand. The service is offered primarily through web-based apps. Mega mobile apps are also available for Android and iOS. Mega is known for its large 50 GB storage allocation for free accounts and will provide additional storage if the user provides a phone number. New Zealand law enforcement has an ongoing working relationship with Mega and has signed a Memorandum of Understanding to allow for information sharing and collaborative investigations involving both New Zealand and international Law Enforcement Agencies.

15. To create a Mega account a user is required to enter a first and last name, email address, password, and password confirmation. The user must verify the selected email address by following a hyperlink contained in an email message they receive from Mega. This

completes the sign-up process. To login to their account a user must enter the email address and password they registered their account with.

16. A user can create links to share access a specific folder, album, or content within their account. The user then shares the links with other users who can view the content without having to log into Mega. Any user that clicks the link can download the files contained in the link since the link includes the decryption key. Additionally, since the link contains the file path and decryption code, any person can simply copy and re-post the link even if they are not the owner of the link.

17. Mega also has private chat rooms that users can create. Users can send links that allow others to access the private chats. These private chats are end-to-end encrypted, so only people who entered the chats via the secure links can see the content. Since a private chat room link contains the file path and decryption code, any person can simply copy and re-post a link even if they are not the owner of the link.

18. The content maintained by Mega is encrypted. Mega cannot access a user's account or view its content without the password or decryption code. Mega does not respond to legal process from the United States but provides basic subscriber records to law enforcement upon request as part of their course of business and in compliance with their terms of service.

19. Cloud storage providers like Mega typically retain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account

via Mega's website or mobile application), number of files contained in the account, data size contained in the account, and other log files that reflect usage of the account. In addition, cloud storage providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the cloud storage account, which can help establish the individual or individuals who had dominion and control over the account. Cloud storage providers like Mega also routinely maintain records of user activity, such as when files are uploaded, shared, or removed.

20. Due to its encryption, Mega has become a popular cloud-based storage repository and/or location to distribute child sexual abuse material. Since Mega does not restrict the same IP address from creating more than one Mega account, persons involved in the receipt, collection, and distribution of child sexual abuse material often have multiple Mega accounts.

21. When a user signs up for a Mega account they explicitly agree to Mega's Limited Terms of Service. Those terms of service notify users that they cannot use Mega to store, use, download, upload, share, access, transmit, or otherwise make available illegal content, including child sexual abuse material, and that Mega can take down an account and disclose unlawful content, including subscriber information, to appropriate authorities.

Background on Mega Emergency Takedown Links (ETD)

22. As discussed previously, a user can create links to share a specific folder, album, or content within their Mega account. The user then shares the links with other users who can view the content without having to log into Mega. Any user that clicks the link can download

the files contained in the link since the link includes the decryption key. When a user clicks the link, that user can observe thumbnails of the shared content. The content is not automatically downloaded into the viewing persons account unless specifically requested by the user.

23. Additionally, since the link contains the file path and decryption code, any person can simply copy and re-post the link even if they are not the owner of the link. The use of links is a common way for content to be shared on Mega and on other social media platforms. These links are unique and can be specifically traced to the Mega account creator including when they created the link or when the link was deactivated.

24. When a user creates and shares a link that contains child sexual abuse material or objectionable material, it is often reported to Mega by other Mega users, the general public, or law enforcement. When the link is reported to Mega as containing child sexual abuse material or objectionable material, Mega deactivates the link and suspends the Mega account that created the link. The content of the links is generally not verified by Mega but are reported as an Emergency Takedown Link or "ETD." Even though the links are deactivated to the general public, the content of the links can be still accessed by Mega and law enforcement. Mega is not aware of what the decryption key is for the link unless it is reported to them.

25. All links created by a Mega account user are documented in the subscriber information for that specific user. It also reflects whether each link is active, deleted, or was suspended as "ETD."

26. A user can only share content that is contained in their Mega account by way of a link. Any content contained in a link created by a Mega user would require that user to have that content in their Mega account. In other words, if the user shared child sexual abuse

material via a Mega link that they created, that user possessed child sexual abuse material in their Mega account.

27. Once Mega flags a link as a "ETD," they then also conduct a "Trace and Strike." Essentially, that is where Mega then identifies any other Mega account that has the specific files that were originally contained in the ETD link. If any other account is identified to have imported files from the original ETD link, that account is also suspended. In my experience, this is typically done to stop the spread of child sex abuse material on their platform.

Statement of Probable Cause

Summary of Investigation

28. In February 2023, HSI, in conjunction with Mayfield Police Department (MPD), initiated an investigation into the online sexual exploitation of at least four minor victims in the greater Mayfield, Kentucky area. In summary, the investigation revealed that at least four minor victims, with ages ranging from 10 to 14 years of age, were using various social media platforms to advertise and sell sexually explicit images and videos of themselves to numerous individuals.

29. One such user was the Instagram user "[redacted]," who was identified as **Gary Anthony MEDEIROS**. **MEDEIROS** used a cell phone that was initially associated with **Former Cell Phone Number-1** ([redacted]) to access Instagram, but I believe he kept the same phone and changed his phone number to **Former Cell Phone Number-2** ([redacted]) in April 2023 and then discontinued the use of this phone in September 2023. **MEDEIROS** is now believed to be using phone number [redacted] (**MEDEIROS' Current Phone Number**). The victims received payment for this content via CashApp, Venmo, and PayPal.[1]

1 Cash App is a mobile payment service available in the United States and elsewhere that allows

MEDEIROS communicated with the minor victims on Instagram from at least March 2022 to January 2023. On at least one occasion, **MEDEIROS** directed Minor Victim-2 (MV-2) to upload her sexually explicit content to his iCloud account, which I believe is [redacted] (**MEDEIROS' iCloud Account**).

30. From at least February 2022 to July 2022, CashApp records reveal that a person believed to be **MEDEIROS** sent approximately $2,000 across 20 different payments to these minor victims. The minor victims sent the sexually explicit media files to **MEDEIROS** primarily using Instagram. The Instagram chats between the victims and **MEDEIROS** were reviewed by law enforcement and are sexual in nature. The chat conversations include discussions regarding the prices for sexually explicit content. After **MEDEIROS** sent the minor victims money, the minor victims would send **MEDEIROS** sexually explicit images and videos via Instagram. All the minor victims were interviewed. It appeared that all minor victims had access to certain social media accounts and were using those accounts interchangeably. Thus, it is hard to say definitively which minor victim was using which social media account at what time.

31. I believe that **MEDEIROS** was located in the District of Oregon and in another unknown District during the commission of the **Target Offense**. According to a review of Instagram messages, it appeared that **MEDEIROS** communicated with the victims and received

---

users to transfer money to others using a mobile phone app. A user creates an account by entering personal information, including their name, date of birth, social security number, phone number, bank account information, and email address. The user then creates a "CashTag," which is a username that is preceded by a dollar sign ($). A user then can send payments to other users by inputting the other user's CashTag.

sexually explicit media files as recently as January 2023 while in the District of Oregon. It is likely that **MEDEIROS** stopped communicating with the minor victims because their digital devices were seized by law enforcement in February 2023.

Victim's Aunt Contacts Police After Discovery of Child Pornography on MV-1's Phone

32. In February 2023, Minor Victim-1's (hereinafter "MV-1") aunt contacted the local police department to report that she found apparent child pornography on MV-1's cell phone.[2] The aunt stated that she discovered the videos after reviewing MV-1's cell phone, which was previously used by MV-1's half-sister, Minor Victim-2 (MV-2).[3]

33. After obtaining consent, law enforcement reviewed MV-1's cell phone. During their review, investigators observed that the phone was signed into an Instagram account with a username that was similar to MV-2's name. MV-1's parents confirmed that the Instagram account in fact belonged to MV-2. Investigators later discovered a second Instagram account belonging to MV-2.

34. Investigators observed that Instagram messages on MV-2's Instagram account included numerous conversations with other Instagram users about the price of producing sexually explicit content followed by sexually explicit images/videos being sent. Many of these sexually explicit media files depicted MV-1, MV-2, and two other minors identified as Minor

2 MV-1 was born in 2011.

3 MV-2 was born in 2008.

Victim-3 (MV-3) and Minor Victim-4 (MV-4).[4] MV-3 and MV-4 are friends with MV-1 and MV-2.

Investigators Obtain a State Search Warrant to Seize MV-2's Digital Devices

35. Based in part on the above information, investigators obtained a state search warrant to seize any digital devices belonging to MV-2 at her residence. During a search, investigators seized an Apple iPad (MV-2's iPad) and an Apple iPhone 14 (MV-2's cell phone). Investigators interviewed MV-2 and she stated that there would be nude images on the iPad. When asked about her activity on Instagram, MV-2 stated, "I would just talk to people on there for money on there, I was selling nudes on there, but my mom already knew about that because that's why she took me to social services."

HSI Joins Investigation and Identifies Instagram User "[redacted]"

36. Due to the multijurisdictional nature of the investigation, state investigators requested the assistance of HSI and turned over MV-1's cell phone and MV-2's cell phone and iPad to HSI. MV-1, MV-1's parents, MV-2, and MV-2's parents subsequently provided written consent for law enforcement to conduct a forensic examination of these three digital devices to assist in the investigation.

37. During a review of these devices and two related Instagram accounts that appeared to belong to MV-2, investigators observed hundreds of sexually explicit media files being sent from MV-2's Instagram account to many other Instagram users.[5] These sexually explicit media files depicted MV-1, MV-2, MV-3, and/or MV-4.

4 MV-3 was born in 2010 and MV-4 was born in 2008.

5 Investigators also obtained federal search warrants for the content of MV-2's Instagram

38. The Instagram chat communications reviewed by investigators included MV-2's Instagram account sending messages regarding various prices for sexually explicit content and inquiring as to what type of content the particular buyer wanted to purchase. After a price was agreed upon, MV-2's Instagram account would send sexually explicit images or videos to the buyer. One such Instagram user was identified as "[redacted]" As discussed in more detail below, this account was identified to be used by **MEDEIROS** who committed the **Target Offense** while in an unknown District and in the District of Oregon.

Investigators Interview Minor Victims

39. When interviewed by investigators, MV-1 stated that MV-2 was taking pictures and videos "fingering herself and stuff" and that MV-2 would send those videos to people for monetary payments through CashApp. When asked about specific videos involving herself, MV-1 stated that she never sent them to anybody, and that MV-2 must have been selling her videos. MV-1 appeared to minimize her involvement. I believe MV-1 to be reliable and credible to the extent that the information she provided has been independently verified by this investigation including through the review of various Instagram and CashApp accounts.

40. When interviewed by investigators, MV-2 stated that she used Instagram and Snapchat to sell nude images/videos of herself to other people in exchange for monetary payments through CashApp. MV-2 stated that she started selling images/videos in 2020 when she was 12 years old. When asked about pricing for her sexually explicit content, MV-2 stated that pictures and videos were $30 and that the pricing did not vary based on if the content

---

accounts. The records provided by Instagram pursuant to the federal search warrants generally are identical to messages obtained during the consent search of MV-1 and MV-2's cell phones.

depicted her buttocks, vagina, or breasts. During the interview, MV-2 appeared to significantly minimize her involvement and stated that another older friend often sold MV-2's photos and videos for money. Additionally, MV-2 claimed that some of her accounts were hacked at times and that it was not her using the accounts during certain time periods. MV-2 also denied that a Twitter account in her name that was identified to be advertising the sale of nude images belonged to her. Subpoenaed records from an IP address that was used to access this Twitter account indicated that the IP address resolved to MV-2's residence. This is consistent with the Twitter account belonging to MV-2. I believe MV-2 to be reliable and credible to the extent that the information she provided has been independently verified by this investigation, including through the review of various Instagram and CashApp accounts. Based on this investigation, it appears that MV-2 was the primary minor victim involved in the solicitation and selling of sexually explicit content.

41. When interviewed by investigators, MV-3 stated that MV-2 was sending pictures and videos of her (MV-3) "naked and doing stuff" to individuals via Instagram, Snapchat, and Twitter. MV-3 stated that MV-2 would receive money in exchange for these pictures and videos of MV-3. MV-3 stated that MV-4 would go to MV-2's house and would send pictures and videos of herself (MV-4) nude in exchange for money. MV-3 stated that MV-2 took a video of MV-3 nude. MV-3 confirmed that sexually explicit images and videos of her were sent to other people via MV-2's Instagram account. MV-3 stated that MV-2 told her not to tell anyone about selling the photos or videos. I believe MV-3 to be reliable and credible to the extent that the information she provided has been independently verified by this investigation, including through the review of various Instagram and CashApp accounts.

42. When interviewed by investigators, MV-4 stated that MV-2 told her that she could make money by selling pictures and videos of herself online via Snapchat and Instagram. MV-4 stated that MV-2 would receive money from selling pictures and videos on CashApp and that they (MV-4 and MV-2) would then use a CashApp debit card to retrieve the money from an ATM. MV-4 stated that MV-2 would provide her with the various social media account information for users who would buy videos and pictures from MV-4. MV-4 stated that MV-2 took the photos and videos of her and the photos and videos were recorded on MV-2's cell phone. MV-4 stated that she had several CashApp accounts that she used to receive money in exchange for the sexually explicit content. When shown some of the sexually explicit videos sent to the Instagram user "[redacted]" (**MEDEIROS**)[6], MV-4 confirmed that it was her in the videos. MV-4 stated she was aware MV-1 and MV-2 were also selling sexually explicit content for money. I believe MV-4 to be reliable and credible to the extent that the information she provided has been independently verified by this investigation, including through the review of various Instagram and CashApp accounts.

*Messages Between MV-2 and Instagram User [redacted] (**MEDEIROS**)*

43. Pursuant to a federal search warrant, investigators obtained message communications, media files, and other records related to MV-2's Instagram account. I have reviewed MV-2's Instagram account records and am familiar with the communications between MV-2 and Instagram user "[redacted]," who I believe to be **MEDEIROS**. These messages spanned from at least March 2022 to January 2023 and were sexually explicit. Numerous

6 Based on the facts outlined in this affidavit, I believe that **MEDEIROS** is the user of the Instagram account [redacted]. As such, I will reference the user as **MEDEIROS**.

images and videos were sent from MV-2's Instagram account to [redacted] (**MEDEIROS**) depicting MV-1, MV-2, MV-3, and MV-4 that I believe meet the federal definition of child pornography. These messages also discussed the payment in exchange for these sexually explicit media files. These payments were then corroborated by CashApp records. I believe that **MEDEIROS** knew the minor victims were under the age of 18 for several reasons including:

a. The physical appearance of the victims depicted in the images and videos sent to **MEDEIROS**' Instagram account. These images and videos depict prepubescent and pubescent-aged girls who a reasonable person would recognize were under the age of 18.

b. In at least one of the videos sent to **MEDEIROS**, MV-3 says she is "13."

c. MV-2 mentions her parents multiple times throughout her Instagram message conversations with **MEDEIROS**, which is consistent with her being under the age of 18.

d. The modus operandi by which the images and videos were purchased. This includes the use of social media accounts primarily used by youth to purchase child sex abuse material.

44. Between March 7 and 18, 2022, MV-2's Instagram account sent **MEDEIROS** several messages, which **MEDEIROS** answered on March 18, 2023. MV-2 asked **MEDEIROS**, "Do you know anyone who buys I really need $200 for my phone :/ Bc I got in a wreck and my phone is messed up :/." MV-2 messaged **MEDEIROS** again and asked, "do you possibly have $200 I could have so I can go get me something for my birthday and get me a

dildo." MV-2 then sent a couple more messages to **MEDEIROS** and he did not respond. It is unclear how or where MV-2 obtained **MEDEIROS**' Instagram account username. However, as further discussed below, CashApp records confirmed that **MEDEIROS** sent money to MV-2 as early as February 2022.

45. On March 22, 2023, MV-2 asked **MEDEIROS** again, "Could I possibly get $200?" **MEDEIROS** did not appear to respond.

46. On June 30, 2022, **MEDEIROS** messaged MV-2 and asked, "Want some $$?" and the following conversation took place[7]:

Author [redacted] (Instagram: [redacted])
Sent 2022-06-30 17:00:16 UTC
Body Want some $$?

Author [redacted] (Instagram: [redacted])
Sent 2022-06-30 17:00:27 UTC
Body Yes

Author [redacted] (Instagram: [redacted])
Sent 2022-06-30 17:01:17 UTC
Body K, ya gonna send me some vids?

Author [redacted] (Instagram: [redacted])
Sent 2022-06-30 17:01:22 UTC
Body [redacted]started a video chat

Author [redacted] Instagram [redacted])
Sent 2022-06-30 17:01:31 UTC
Body You missed a video chat

Author [redacted] (Instagram: [redacted])
Sent 2022-06-30 17:01:45 UTC
Body Yes

Author [redacted] (Instagram: [redacted])
Sent 2022-06-30 17:01:48 UTC
Body If you send

Author [redacted] (Instagram: [redacted])
Sent 2022-06-30 17:01:52 UTC
Body [redacted]

Author [redacted] Instagram: [redacted])
Sent 2022-06-30 17:04:17 UTC
Body Sent u 50 for now, I'll send more if ya earn it

Author [redacted] (Instagram: [redacted])
Sent 2022-06-30 17:10:23 UTC
Body Yoo

Author [redacted] (Instagram: [redacted])
Sent 2022-06-30 17:11:23 UTC
Body You want more $$?

Author [redacted] (Instagram: [redacted])
Sent 2022-06-30 18:05:53 UTC
Body Yoo

Author [redacted] Instagram: [redacted])
Sent 2022-06-30 18:06:20 UTC
Body I prob got another $100 for you

Author [redacted] (Instagram: [redacted])
Sent 2022-06-30 18:06:31 UTC
Body Okay

Author [redacted] (Instagram: [redacted])
Sent 2022-06-30 18:07:01 UTC
Body Ya gotta send me some vids though for that 50 first

Author [redacted] (Instagram: [redacted])
Sent 2022-06-30 18:07:08 UTC
Body Okay add my snap first

Author [redacted] Instagram: [redacted])
Sent 2022-06-30 18:08:17 UTC
Body You can't just send it here?

Author [redacted] (Instagram: [redacted])
Sent 2022-06-30 18:09:19 UTC
Body no

Author [redacted] (Instagram: [redacted])
Sent 2022-06-30 18:11:33 UTC
Body Ok

7 To protect her identity, MV-2's Instagram username and CashTag were redacted in these messages.

47. MV-2 then sent a series of photographs that depicted her in various stages of undress, including showing her bare buttocks and breasts. One of the photographs displayed presumably MV-2's vagina. The focal point of the photograph was MV-2's vagina, which I believe meets the federal definition of child pornography. In many of the photographs MV-2's face was clearly visible. **MEDEIROS** then told MV-2 to "send more vids babe…Lemme see more of your [box emoji]." Based on the context and the box emoji, I believe that **MEDEIROS** was telling MV-2 to send videos of her vagina. **MEDEIROS** then told MV-2 that he had more money he wanted to spend and sent a screenshot of his online bank account that read $358.27. MV-2 told **MEDEIROS** to send more money and **MEDEIROS** responded by saying, "Nah I'm not playing that game…You do that shit every time I have tried to buy from you and you always try n get more and more n don't end up sending more."

48. MV-2 then sent a video to **MEDEIROS** that depicted MV-2 in a bathroom. In the video, MV-2 pulls down her underwear and exposes her vagina. - MV-2 then zooms the camera in on her vagina. **MEDEIROS** told MV-2 to "Make me a couple longer vids later."

49. MV-2 sent another video that depicted her pulling down her pants, getting onto her knees, and spreading her anus and vagina for the camera. MV-2 proceeded to send **MEDEIROS** additional videos and images that I believe met the federal definition of child pornography. I believe MV-2 sent these in exchange for the money **MEDEIROS** sent her. **MEDEIROS** then said, "I want more pussy and more dirty talk babe." MV-2 then sent a video that depicted MV-3. In the video, MV-3 is naked and standing in what appears to be a bathroom. MV-3 says, "fuck me daddy I am 13" and then brings the camera to her vagina. I believe the reference to "13" is in fact MV-3's age. **MEDEIROS** asked MV-2 who the girl

(MV-3) was in the video and MV-2 explained that she was her friend and that she was sending additional videos.

50. Over the next several hours, MV-2 sent **MEDEIROS** dozens of videos and images that meet the federal definition of child pornography and that depict MV-1, MV-2, MV-3, and MV-4. When he was questioned by MV-2 about whether he sent money or not, **MEDEIROS** sent two screenshots that showed $100 sent to MV-2's CashApp account from an account with the CashTag [redacted]. A review of the transactions for [redacted] revealed 14 transactions to a CashApp account in the name of MV-2 totaling $1,450. As discussed further below, the account [redacted] is registered in the name of "[redacted]" but has various iterations of **MEDEIROS**' name for the display name including "Gary" and "g.a." Additionally, the user of CashApp account [redacted] updated their address on August 31, 2022, to 875 SW 158th Ave, Beaverton, OR 97006. This address is an Extended Stay America hotel where **MEDEIROS** was residing at times during the time period of at least October 2022 to April 2023 . As such, I believe that the CashApp account [redacted] is in fact used by **MEDEIROS**.

51. In July 2022, MV-2 and **MEDEIROS** continued to engage in sexually explicit communications. It is currently not known exactly where **MEDEIROS** was located during this time period. IP logs received from Instagram reflect a cellular phone IP address with a general location of Los Angeles, California and another cellular phone IP address with a general location of North Carolina. I know based on my training and experience that open-source inquiries of cellular phone IP addresses can often be unreliable. Additionally, based on the investigation I have uncovered no additional records such as utility records, travel documents, hotel records, IP

addresses subscribed to physical locations, or anything else to establish definitively where **MEDEIROS** was during this time period.

52. Between July 5, 2022, and September 4, 2022, MV-2 messaged **MEDEIROS** several times, but **MEDEIROS** did not appear to respond.

53. On November 29, 2022, **MEDEIROS** messaged MV-2 "hi," to which MV-2 responded "Hey." **MEDEIROS** explained that he had a lot of things going on and MV-2 asked "You trynna spoil me?" to which **MEDEIROS** said, "Maybe a little rn [right now]." MV-2 then directed **MEDEIROS** to send money to a CashApp account and provided the account's CashTag, which included a partial name of one of the minor victims. **MEDEIROS** asked, "Are you gonna make me cum," and MV-2 replied, "Yes if you send." MV-2 then asked for $100 and **MEDEIROS** stopped responding. Over the next several weeks, MV-2 and **MEDEIROS** exchanged several benign messages.

54. On January 9, 2023, MV-2 provided **MEDEIROS** with a PayPal account in the name of [redacted] and told **MEDEIROS** to "spoil me."[8] **MEDEIROS** told MV-2 that he was driving and challenged her to send him something that would "make [him] pull over." MV-2 then sent several pictures and videos that depicted her naked in the shower. In some of the videos her vagina is visible. MV-2 then asked, "Are you sending now," and **MEDEIROS** told her that he was having some problems. MV-2 told **MEDEIROS** that she could accept payment via CashApp, Apple Pay, and Venmo. **MEDEIROS** stopped responding

8 Investigators have identified "[redacted]" as a real individual that lives approximately 30 minutes away from the minor victims, who is an adult (xx/xx/2003). I am not aware that investigators have interviewed [redacted] as of the date of this application.

to MV-2. As discussed further below, I believe **MEDEIROS** was located in the District of Oregon during the above conversation and continued to commit the **Target Offenses**.

55. On January 14, 2023, MV-2 again messaged **MEDEIROS** saying, "can I send ass spread v," to which **MEDEIROS** replied, "You're full of shit lol. If you want me to send more money, then make me a video fully naked, legs spread, playing with your pussy for like 5 min." MV-2 then explained to **MEDEIROS** that she could not send videos that long on Instagram. **MEDEIROS** provided her with step-by-step instructions and screenshots on how to share a video via an iCloud link (which would not have size restrictions), which I believe is likely **MEDEIROS**' iCloud Account. **MEDEIROS** went on to explain "it's pretty simple, I just wanna cum n you keep dragging this out and stalling and making excuses saying you're gonna send….like if you send the vid I'll respond, but you better moan my fucking name while you play with that pussy now." MV-2 told **MEDEIROS** that she could not "finger" but could "play with it." **MEDEIROS** then said, "You literally scammed me lol." As discussed above, the minor victims' digital devices were seized by law enforcement in February 2023.

56. During a review of Instagram connectivity records for Instagram user [redacted] (**MEDEIROS**), I learned that the account utilized IP address [redacted] five times between November 28, 2022, and February 15, 2023. According to subpoenaed records from Comcast, IP address [redacted] was subscribed to Extended Stay America located at 875 SW 158th Ave, Beaverton, OR 97006. As further described below, **MEDEIROS** rented numerous rooms at this hotel during this time period. This IP connectivity is consistent with the user of Instagram account [redacted] being **MEDEIROS**. As such, I believe **MEDEIROS** was located within the District of Oregon during this time period when he committed the **Target Offense**.

57. According to subpoenaed records from Extended Stay America and as further discussed below, I learned that **MEDEIROS** rented rooms at this location numerous times from at least October 2022 to April 2023. These rooms were rented in his first and last name and he also provided a copy of his Oregon Driver's License to the front desk. I showed a photograph of **MEDEIROS** to the manager of this Extended Stay America, who immediately recognized him. The manager confirmed that **MEDEIROS** essentially lived at the motel from October 2022 to April 2023.

*Investigators Identify **MEDEIROS** as Instagram User* [redacted]

58. According to subpoenaed records from Instagram, the user "[redacted]" was created on January 28, 2021, had a verified phone number of [redacted] (**Former Cell Phone Number-1**), and listed the user's name as "gary." As further discussed below, **MEDEIROS** replaced **Former Cell Phone Number-1** with **Former Cell Phone Number-**2 on April 23, 2023. The phone number [redacted] (**Former Cell Phone Number-1**) was "verified," which means that the user responded to a communication from Instagram verifying that they were in possession of the cell phone associated to that number. Therefore, I believe that **MEDEIROS** was in possession of and used the cell phone assigned **Former Cell Phone Number-1**.

59. Instagram also provided IP access records from March 15, 2021, to March 15, 2023. During a review of these logs, I observed approximately 39 logins between October 3, 2021, and February 15, 2023, most of which were IP addresses resolving to T-Mobile. Specifically, approximately 34 of the 39 IP addresses appeared to resolve to T-Mobile, which is consistent with the use of a cell phone. The remaining five logins occurred between November

28, 2022, and February 15, 2023, and utilized IP address [redacted]. Based on my training and experience, Instagram records a login event each time the account is logged into. As such, if the user stays signed into the account on a specific device Instagram does not capture each instance the user accesses the account.

60. According to subpoenaed records from Comcast, IP address [redacted] was subscribed to 875 SW 158th Ave, Beaverton, OR 97006, which was identified to be an Extended Stay America hotel in Beaverton, Oregon. As discussed above, **MEDEIROS** was confirmed to stay at this location numerous times, including between October 31, 2022, and April 9, 2023. This is consistent with **MEDEIROS** being the user of the Instagram account "[redacted]." Additionally, the Instagram account "[redacted]" displayed a cropped picture of a male wearing sunglasses that I recognize to be **MEDEIROS**. I am familiar with the appearance of **MEDEIROS** from reviewing his Oregon Driver License and body camera footage from police contact that occurred in Union City, California on May 15, 2023.

61. According to subpoenaed records from CashApp, phone number [redacted] (**Former Cell Phone Number-1)** and the phone number for Instagram user [redacted]) was assigned to an account in the name, date of birth, and social security number (last four digits) of **MEDEIROS**. This is a different CashApp account than the one in the name of "[redacted]" as described above. Also associated with this account were several email addresses including [redacted] (**MEDEIROS**' iCloud Account), and [redacted] and phone number [redacted].[9]

9 There was another name, date of birth, and social security number associated to the account that "failed to verify," which was "[redacted]" with date of birth xx/xx/94. I was unable to find a real person with this name and date of birth. Additionally, the name "[redacted]" is sexually

62. According to subpoenaed records from Google, email address [redacted] and [redacted] both had connectivity from the same IP address that was subscribed to the Extended Stay America during the time period **MEDEIROS** was identified to rent rooms there. This is consistent with **MEDEIROS** being the user of both those email addresses. Of note, email address [redacted] had a recovery phone number of [redacted] (i.e., the same phone number as listed on **MEDEIROS**' CashApp account) but also a recovery email address of [redacted]. I know based on my training and experience that the @me.com mail domain is an email account that is associated with the Apple iCloud service. This type of account allows you to access your email from mobile devices and desktop email clients. I believe that [redacted] is simply a mail domain overlay for **MEDEIROS**' iCloud Account, which I believe is [redacted]. As further discussed below, **MEDEIROS** specifically explained to MV-2 how to upload child sex material to an iCloud account, which I believe is **MEDEIROS**' iCloud Account. The namesake email address of [redacted] is also consistent with several of **MEDEIROS**' online personas, which involve various naming conventions including the word "gary" and "danger." I also know based on my training and experience, and facts in this investigation, that **MEDEIROS** has spent large sums of money to obtain the child sex abuse material and would continue store, collect, and revisit those images and videos. As such, I believe that there is likely evidence in **MEDEIROS** iCloud account.

---

suggestive. As such, I believe that it was likely a fictitious identity used by **MEDEIROS**.

63. The CashApp account also had several display names associated to it including "Gary M," "Vanessa cox," "Vanessa," "Christopher **MEDEIROS**," "Gary A," "Gary **MEDEIROS**," and "Kierstyn." The reported address of this CashApp account was [redacted] and [redacted]. According to Oregon DMV records, **MEDEIROS**' reported address is [redacted] (**Subject Premises**).

64. Subpoenaed records from T-Mobile reflected that phone number [redacted] (**Former Cell Phone Number-1** and the phone number for Instagram user [redacted]) was subscribed to "Christopher MEDEIROS" at the **Subject Premises** and had IMEI number [redacted]. It appeared that the phone number changed subscribers on January 24, 2023, to "Deborah **MEDEIROS**" at the same address. Based on this, I believe it is likely that **MEDEIROS**' family members were paying for the cell phone assigned **Former Cell Phone Number-1** for **MEDEIROS**. Additionally, phone number [redacted] (i.e., a phone number on **MEDEIROS**' CashApp and Gmail account) was subscribed to "G M" at [redacted] (**Subject Premises**). "G M" are **MEDEIROS**' initials. As further discussed below, I believe that **MEDEIROS** stopped using phone number [redacted] (**Former Cell Phone Number-1**) in April 2023 and began using phone number [redacted] (**Former Cell Phone Number-2**). **MEDEIROS** then discontinued the use of **Former Cell Phone Number-2** in September 2023 and is now believed to be using phone number [redacted] (**MEDEIROS' Current Phone Number**). Records from T- Mobile confirmed that **MEDEIROS** kept the same cell phone (i.e., cell phone with IMEI [redacted]) but simply changed phone numbers between **Former Cell Phone Number-1** and **Former Cell**

Phone Number-2. I have served a subpoena on Verizon Wireless for records related to **MEDEIROS' Cell Phone Number** and have not received a response yet. Therefore, I currently do not know if **MEDEIROS** still has the same physical device as his former phone numbers.

65. During a review of the payments from this CashApp account, I observed that between January 3 and February 3, 2022, **MEDEIROS** sent seven payments to an account in the name of MV-2 totaling $740. This is consistent with **MEDEIROS** having previous communications with MV-2 and purchasing additional sexually explicit videos that are not presently known to law enforcement.

66. I also reviewed the "Subject" section related to the CashApp transactions on **MEDEIROS**' various accounts for outgoing payments. The "Subject" section is a place where the sender (i.e., **MEDEIROS**) can write a note that the recipient of the money will see. In reviewing these notes, I observed many that were sexually suggestive and also where **MEDEIROS** appeared to provide other social media accounts that the recipient could contact him on. I also observed that **MEDEIROS** sent similar payments (i.e., dollar amount and "Subject" notes) to many other CashApp accounts that were not in the name of any of the minor victims in this case. These payments are likely for sexually explicit content from other individuals. For example:

a. On September 8, 2022, **MEDEIROS** sent a payment to "[redacted]" that read "come onnn I got a lot more $$ for you."

b. On August 31, 2022, **MEDEIROS** sent a payment to "[redacted]" that read "hiii ;) tryin to sell to me? 😉😉."

c. On August 23, 2022, **MEDEIROS** sent a payment to "[redacted]" that read "send me some contenttt 😉😉. 👻👻[redacted]" Based on my training and experience, I believe the reference to "content" is in fact asking for sexually explicit content. **MEDEIROS** then provided the Snapchat account "[redacted]."

d. On June 4, 2022, **MEDEIROS** sent a payment to "[redacted]" that read "tits n ass from last night if u want $$$ lol."

e. On May 18, 2022, **MEDEIROS** sent a payment to "[redacted]" that read "hiiii…. make me 🥜🥜 plz😈😈." I know based on my training and experience that the "nut" emoji is in reference to **MEDEIROS** ejaculating.

f. On March 20, 2022, **MEDEIROS** sent another payment to "[redacted]" with a note that read "now it's your turn to send something lol."

//

//

//

//

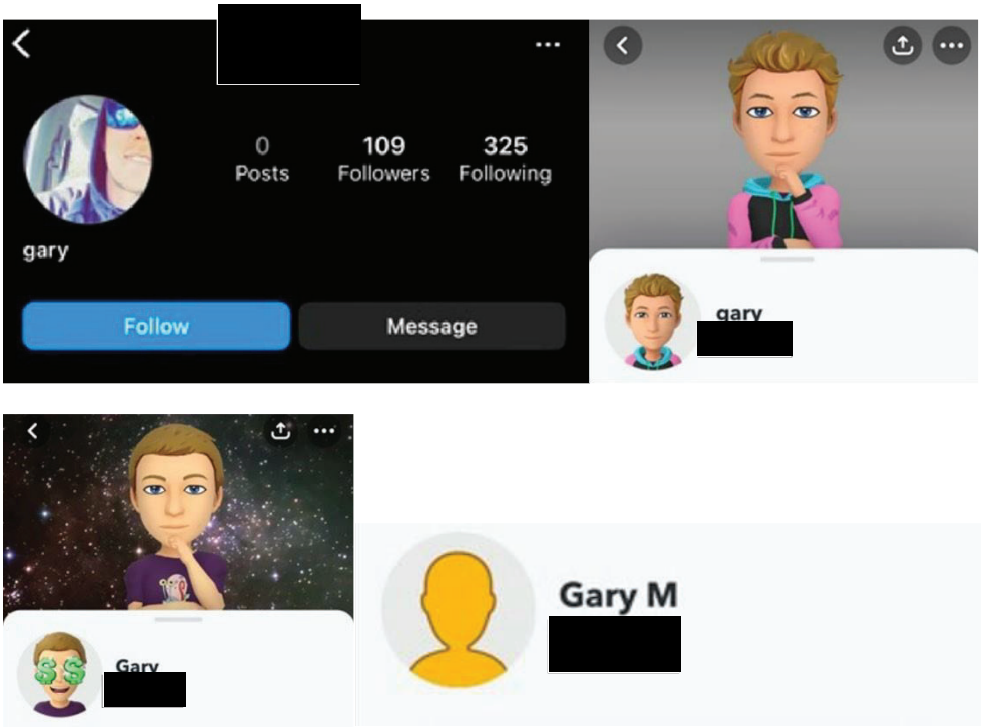
//

//

//

//

67. These are just several examples of the payment activity from **MEDEIROS**' CashApp accounts. It appeared that **MEDEIROS** also used the "Subject" section of the payments to provide additional social media accounts that he presumably uses. These accounts included the following accounts: [redacted]. I searched on Snapchat and Instagram and located that several of these usernames had corresponding accounts as follows:



68. According to additional IP logs obtained from a CashApp account that I believe was used by **MEDEIROS**, I observed that **MEDEIROS** used the same IP address ([redacted]) as the Instagram account [redacted] As discussed above, this IP address was subscribed to the Extended Stay America in Beaverton, Oregon. The Instagram account [redacted] was used to receive hundreds of sexually explicit images and videos of MV-1, MV-2, MV-3, and/or MV-4 between at least June 2022 and January 2023. CashApp records confirmed

that **MEDEIROS** accessed his CashApp account numerous times using this IP address between August 2 and October 4, 2022. This is again consistent with **MEDEIROS** being in the District of Oregon between at least August 2, 2022, to April 8, 2023, when he eventually stole a car and fled to California.

Investigators Identify that MEDEIROS Stole a Rental Car and Fled to California

69. According to law enforcement inquiries, I learned that **MEDEIROS** had rented a car from Enterprise on April 8, 2023, from the Portland International Airport. **MEDEIROS** originally rented the car for a one-day rental to be returned in Oakland, California but extended the rental until April 16, 2023. Several days later, Enterprise reported the car stolen when **MEDEIROS** did not return the car or respond to any correspondence from Enterprise.

70. According to the police report from Portland Police Bureau (PPB), **MEDEIROS** reported on the car rental agreement that his phone numbers were [redacted] and [redacted] and that his address was [redacted] (**Subject Premises**). Of note, the phone number [redacted] is almost the exact number for the Instagram user [redacted] (i.e., **Former Cell Phone Number-1**). I believe that **MEDEIROS** or the car company inadvertently mixed up the last two numbers of the phone number when he rented the car. PPB and Enterprise attempted to contact **MEDEIROS** using the provided phone numbers but they were no longer active; presumably because they had the wrong phone number by one digit. PPB then entered the vehicle as stolen and disseminated this notification to the law enforcement community. Based on the above information, PPB also issued a warrant for **MEDEIROS**' arrest on various state law violations for vehicle theft.

71. According to law enforcement databases, I learned that on May 15, 2023, a Crowne Plaza hotel in Union City, California contacted the police department to report an occupant who had an unauthorized animal in their hotel room. The hotel guest was later identified as **MEDEIROS**. Union City Police Department (UCPD) responded and learned that **MEDEIROS** had an outstanding warrant from PPB related to the theft of the rental vehicle. **MEDEIROS** was cited with a court date to appear pursuant to this warrant, which was set for June 12, 2023. **MEDEIROS** provided phone number [redacted] (**Former Cell Phone Number-2**) and stated that his address was [redacted] (**Subject Premises**). **MEDEIROS** failed to show up for his court appearance and a bench warrant was issued for his arrest, which is still outstanding.

72. According to subpoenaed records from T-Mobile, I learned that phone number [redacted] (**Former Cell Phone Number-2**) was subscribed to "Gary **MEDEIROS**" and was activated on April 23, 2023. The change in phone numbers between **Former Cell Phone Number-1** and **Former Cell Phone Number-2** is consistent with when **MEDEIROS** stole the rental car from Enterprise. While reviewing the records I also learned that even though **MEDEIROS** changed his phone numbers the cell phone device appeared to be the exact same cell phone. I formed this conclusion based on the fact that the IMEI number stayed the same ([redacted]) after the phone numbers changed. As described above, **MEDEIROS** discontinued the use of **Former Cell Phone Number-2** in September 2023 and is now believed to be using phone number [redacted] (**MEDEIROS' Current Phone Number**). I have served a subpoena on Verizon Wireless for records related to **MEDEIROS' Cell Phone**

Number and have not received a response yet. Therefore, I currently do not know if **MEDEIROS** still has the same physical device as his former phone numbers.

Investigators Identify Cloud-Based Storage Accounts Linked to MEDEIROS that Contain Child Pornography

73. Suspecting that **MEDEIROS** likely had additional cloud-based storage, I sent a request to Mega inquiring if there were any accounts associated to various email addresses including [redacted]. This is an email address reported on a CashApp account believed to have been used by **MEDEIROS**.

74. According to records obtained from Mega, I learned that there was an account associated to email address [redacted] that was created on March 5, 2021, and last accessed on February 9, 2023, when it was closed by Mega for containing suspected child pornography. The user self-reported their name as "Ew Aqed" and provided phone number [redacted]. As discussed above, the phone number [redacted] was subscribed to "GM" at the **Subject Premises**, was reported as a recovery phone number on one of **MEDEIROS's** email accounts [redacted]), and was listed as a phone number on a CashApp account attributable to **MEDEIROS**.

75. The records obtained from Mega also indicated that the account had approximately 97,974 files, which was approximately 1,600 gigabytes of data. This is consistent with the massive downloading of files. I also observed that the account was a premium account and the user paid a monthly subscription fee for increased storage capacity and was primarily accessed from an iPhone 12 Pro Max.

76. According to a review of IP connectivity logs, I observed that the Mega account was accessed numerous times from various IP addresses including T-Mobile and Comcast. Of note, I observed that the account was accessed several times from IP address [redacted]. As discussed above, this IP address was subscribed to the Extended Stay America hotel where **MEDEIROS** was residing while in the District of Oregon from at least October 2022 to April 2023. The account was accessed from this IP address on at least: February 9, 2023, and December 7, September 13, August 29, August 7, August 5, and August 1, 2022. This is consistent with **MEDEIROS** being in the District of Oregon at those times and accessing his Mega account.

77. In reviewing the records provided by Mega, I also learned that the account was suspended for importing suspected child pornography from various public links on the Mega platform and that those files still existed in the account until it was suspended in February 2023. These are flagged as "ETD" or "Emergency Takedown." Since the links were public, Mega had access to the links, preserved the content of each link, and subsequently suspended each link. If requested by law enforcement, Mega provides the content of each link to law enforcement to further investigations.

78. I sent a request to New Zealand Department of Internal Affairs (NZ DIZ) requesting a sampling of the identified files that were imported into **MEDEIROS'** Mega account. NZ DIA has a Memorandum of Understanding with Mega and acts as law enforcement liaison on behalf of Mega to fulfill international requests for records.

79. In October 2023, I received a random sampling of 20 files that were identified as suspected child pornography that were contained in **MEDEIROS'** Mega account up until the

account was suspended in February 2023. In reviewing these media files, I believe that all 20 meet the federal definition of child pornography. For example:

- File Name: [redacted].jpg / File ID: [redacted]
    a. Date Imported: December 12, 2021
    b. Description: An image that depicted a child, approximately 7 – 10 years of age, licking an adult male's penis.
- File Name: [redacted]mp4 / File ID: [redacted]
    a. Date Imported: July 12, 2022
    b. Description: A video that depicted a prepubescent female child, approximately 3 – 5 years of age, naked and using the bathroom. An adult male then ejaculates into the child's mouth. The child is crying.
- File Name: [redacted].jpg / File ID: [redacted]
    a. Date Imported: July 13, 2022
    b. Description: An image that depicted a pubescent female child, approximately 11 – 13 years of age, lying naked with her vagina pointed towards the camera. The child is using her hands to spread her vagina.

80. Based on the above, I believe that **MEDEIROS** had a Mega account that contained child pornography. I believe that he possessed and accessed this account multiple times while in the District of Oregon between at least August 1, 2022, to February 9, 2023, when it was suspended by Mega. Based on my training and experience, and conversations with NZ

DIA, I am aware that even though **MEDEIROS'** Mega account has been suspended it can be accessed if law enforcement is able to locate his password.

*Investigators Obtain a Federal Search Warrants to "Ping" **MEDEIROS'** Cell Phone and for Historical Cell Site Data*

81. On September 28, 2023, based in part on the above information, the Honorable Youlee Yim You, United States Magistrate Judge, District of Oregon, signed search warrants authorizing law enforcement to obtain historical cell tower records and/or GPS location data for **Former Cell Phone Number-1** and **Former Cell Phone Number-2**. These warrants were assigned case numbers [redacted]

82. After serving the warrants, investigators learned that **MEDEIROS** discontinued the use of **Former Cell Phone Number-2** several days prior to the warrant being signed, and investigators obtained no real-time location data. T-Mobile has not provided the historical records for **Former Cell Phone Number-1** yet.

Request for Sealing

83. I request that the Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested criminal complaint and arrest warrant. I believe that sealing these documents is necessary because the information to be seized is relevant to an ongoing investigation, and any disclosure of the information at this time could cause flight from prosecution and/or otherwise seriously jeopardize an investigation. Premature disclosure of the affidavit, the criminal complaint, and the arrest warrant may adversely affect the integrity of the investigation.

//

Conclusion

84. Based on the foregoing, I have probable cause to believe that **Gary Anthony MEDEIROS** committed violations 18 U.S.C. § 2252A(a)(2) – *Receipt of Child Pornography* (**Target Offense**). I therefore respectfully request that the Court issue a criminal complaint and arrest warrant charging **MEDEIROS** with that offense.

85. Prior to being submitted to the Court, this affidavit, the accompanying complaint, and the arrest warrant were all reviewed by Assistant United States Attorney Charlotte Kelley. AUSA Kelley advised me that in her opinion, the affidavit is legally and factually sufficient to establish probable cause to support the issuance of the requested criminal complaint and arrest warrant.

/s/ Clinton Lindsly By telephone
CLINTON LINDSLY
Special Agent
Homeland Security Investigations

Sworn to before me telephonically or by other reliable means pursuant to Fed. R. Crim. P. 4.1 at 4:20 pm am/pm on October 25, 2023.

Youlee Yim You
HONORABLE YOULEE YIM YOU
United States Magistrate Judge